SYSTEM AND METHOD FOR PROTECTING A TITLE KEY IN A SECURE DISTRIBUTION SYSTEM FOR RECORDABLE MEDIA CONTENT

FIELD OF THE INVENTION

[0001] The present invention generally relates to a system for encrypting copyrighted content such as music or movies. More specifically, the present invention pertains to a method for protecting a title key of content by eliminating the need to store that title key in a repository database, protecting such content from unauthorized use or distribution.

BACKGROUND OF THE INVENTION

[0002] The entertainment industry is in the midst of a digital revolution. Music, television, and movies are increasingly becoming digital, offering new advantages to the consumer in quality and flexibility. At the same time the digital revolution also comprises a threat since digital data can be perfectly and quickly copied. If consumers may freely copy entertainment content and offer that content on the Internet, the market for entertainment content would evaporate.

[0003] The rapid growth in the distribution of recordable media over the Internet, such as MP3s and DVDs, is especially alarming to content owners. These highly controversial and unauthorized distribution channels have caused an increase in demand from the entertainment industry for methods to protect their multi-million dollar content. Developing a content protection system that offers content owners an end-to-end solution they can use to securely distribute their media is becoming increasingly important as the amount of content shared across the Internet grows exponentially each year.

[0004] Recently, developments in consumer electronics have created an alternative to traditional digital rights management systems. New recording and playing devices that use this new method, known as CPRM (Content Protection for Recordable Media) technology, have reached the market. It is now possible to directly record content protected in CPRM to writable media. If the recording is prepared in a server the client needs no special keys or tamper-resistance. This method of content protection utilizes broadcast encryption. Devices do not need to have a conversation to establish a common key. Recent advances in broadcast encryption have made it as powerful as public-key cryptography in

terms of revocation power. Because of its one-way nature, broadcast encryption is inherently suited to protect content on storage.

[0005] Once the client receives the encrypted recordable media content using CPRM, the interaction between the content server and the client side module is complete. The server is now free to focus on other requests. On the client side, CPRM requires that the encrypted content be recorded onto a physical piece of media, such as a DVD. This recording is performed in such a way that the encrypted content can only be played by a compliant device while it is on that particular piece of media. Consequently, encrypted content copied to another physical piece of media cannot by played by a compliant device.

[0006] CPRM devices use the media key block and media ID located currently on blank DVD recordable disks to calculate a media unique key. The media unique key is used to encrypt title keys. In turn, the title keys encrypt the content stored on the DVDs. Encrypting the title keys in the media unique key causes the title keys to become cryptographically bound to the particular piece of physical media on which the content is burnt. This prevents the content from being decrypted and accessed from any other physical piece of media.

[0007] Although this technology has proven to be useful, it is desirable to present additional improvements. In a server-based CPRM system, the calculation that binds the title key to the media is performed on the server-side, not the client-side. However, there is currently no means by which the server may learn the title key other than storing the title key in a database. Such a database is difficult to maintain in a secure and tamper-resistant environment.

[0008] What is therefore needed is a system, a computer program product, and an associated method for protecting a title key while providing means for

the clearinghouse server to learn the title key. The need for such a solution has heretofore remained unsatisfied.

SUMMARY OF THE INVENTION

[0009] The present invention satisfies this need, and presents a system, a computer program product, and an associated method (collectively referred to herein as "the system" or "the present system") for including the title key with recordable media content in such a manner that storage in a repository is not required. Rather, the title key is decrypted when needed by a clearinghouse, and then re-encrypted. The title key confers rights from the content owners to the user to play and copy the content for personal use. Without a title key, a media recording device will neither play nor copy the recordable media content.

[0010] Using the present system, a user purchases encrypted recordable media content from a content provider through a content repository. This recordable media content is downloaded to the user's media recording device. The user's media recording device extracts an encrypted title key from the recordable media content. The media recording device also obtains a media key block and media ID from the physical media on which the recordable media content will be recorded. The encrypted title key is transmitted to a clearinghouse along with the media key block and the media ID. The clearinghouse decrypts the title key and derives a media unique key from the media key block and media ID. The clearinghouse then re-encrypts the title key with the media unique key, creating a re-encrypted title key for recording on the physical media. This re-encrypted title key is unique to the physical media. The re-encrypted title key provides authorization required by the media recording device to play the recordable media content that has been recorded on the physical media.

[0011] The present system uses a media key block to encrypt and decrypt the title key. Each media player has a unique set of keys that allow the media

player to process the media key block; however, each device follows a unique path through the media key block. All legitimate devices end up with a media key as the result of the decryption. However, if circumvention devices appear, newly released physical media can be manufactured so that the circumvention devices, following their particular paths through the media key block, get the wrong answer. All innocent devices continue to correctly calculate the media key. Consequently, only the circumvention devices are excluded from the system.

[0012] The present system uses the media key block on the physical media as an aid to deliver content keys across the Internet, thereby avoiding a single global secret. A web service provider or other processing center delivers an encrypted title key across the Internet. Possession of the correctly encrypted title key by the user verifies that a user has received the right to play and record the recordable media content. Consequently, content owners wish to protect the title keys for their content. Rather than store the title key, the present system provides a method by which the title key can be decrypted when needed.

[0013] The clear advantage of the present system is that a database is not required by a clearinghouse to store title keys for content. Even if it has not seen a particular piece item of content before, the clearinghouse is able to decrypt the title key. The clearinghouse can then re-encrypt the title key in the media unique key specific to the physical media on which the content will be recorded. Using the present system, only the processing of the title key is required to be secure and tamper-resistant. Secure processing is well within the current art; however, databases storing title keys are targets for attacks and difficult to keep secure, especially when the clearing house must act on behalf of several different content owners who are competitors, each needing to store their own keys.

[0014] The present system provides a level of abstraction away from the actual encrypted content, eliminating interaction between the clearinghouse and the content repository that stores the content. Consequently, the clearinghouse is less complex than a full content repository and can be placed anywhere that is accessible by a media recording device such as a DVD player. The clearinghouse is not tied to a database or content repository location.

[0015] In addition, the clearinghouse server and the content repository server may be completely independent, allowing deployment of additional business models. For example, the content owners may operate the content servers while an electronic retail store may operate the clearinghouse.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The various features of the present invention and the manner of attaining them will be described in greater detail with reference to the following description, claims, and drawings, wherein reference numerals are reused, where appropriate, to indicate a correspondence between the referenced items, and wherein:

[0017] FIG. 1 is a schematic illustration of an exemplary operating environment in which a title key protection system of the present invention can be used;

[0018] FIG. 2 is a block diagram of the high-level architecture of the title key protection system of FIG. 1;

[0019] FIG. 3 is comprised of FIGS. 3A and 3B and represents a process flow chart illustrating a method of operation of the title key protection system of FIGS. 1 and 2; and

[0020] FIG. 4 is a process flow chart illustrating an embodiment of a method of the title key protection system of FIGS. 1 and 2 in transmitting a media key block.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0021] The following definitions and explanations provide background information pertaining to the technical field of the present invention, and are intended to facilitate the understanding of the present invention without limiting its scope:

[0022] Internet: A collection of interconnected public and private computer networks that are linked together with routers by a set of standard protocols to form a global, distributed network.

[0023] World Wide Web (WWW, also Web): An Internet client - server hypertext distributed information retrieval system.

[0024] Content: copyrighted media such as music or movies presented in a digital format on electronic devices.

[0025] FIG. 1 portrays an exemplary overall environment in which a system and method for protecting a title key in a secure distribution system for recordable media content according to the present invention may be used. A title key protection system 10 comprises a software programming code or a computer program product that is typically embedded within, or installed on a media playing device 80, a clearinghouse server 20, and a content repository 25. Alternatively, the title key protection system 10 can be saved on a suitable memory or storage medium such as a diskette, a CD, a DVD, a hard drive, or like devices.

[0026] Content repository 25 comprises a content repository server 30 and recordable media in the form of content 35. Content 35 comprises any

recordable media such as, for example, a software program, music, a movie, a game, a book, etc. A clearinghouse 40 comprises the clearinghouse sever 20. Clearinghouse 40 and content repository 25 may be part of the same content providing entity. Conversely, clearinghouse 40 and content repository 25 may be separate entities. For example, content owners may operate content repository 25 while a third party retailer may operate clearinghouse 40.

[0027] The media recording device 15 can access the clearinghouse server 20 and the content repository server 30 through a network 45. The media recording device 15 comprises software that allows the media recording device 15 to interface securely with the clearinghouse server 20 and the content repository server 30. The media recording device may be a personal computer with appropriate software and hardware, or it may be a special purpose device such as a DVD video recorder.

[0028] The media recording device 15 is connected to network 45 such as the Internet via a communications link 50 such as telephone, cable, DSL, satellite link, etc. The clearinghouse server 20 is connected to the Internet through a communications link 55 and the content repository server 30 is connected to the Internet through a communications link 60.

[0029] The media playing device 80 can comprise any compliant module that can verify the physical presence of media such as, for example, a disc. A compliant module is one that follows the usage rules that are cryptographically bound to content downloaded from content repository server 30. Media playing devices 80 comprise, for example, computers, DVD players, game players, etc.

[0030] A user may download content 35 from the content repository server 30 to the media recording device 15, which records it on physical media 65.

Content 35 may be purchased, rented, or provided free of charge by content repository 25. The user may wish to play content 35 on media playing device 80, using the physical media 65. The physical media 65 comprises a media key block 70 and a media ID 75 that have been inserted in the physical media 65 when manufactured. In some cases, the media recording device 15 and the media playing device 80 may be the same physical device with both recording and playing functions.

[0031] The content repository server 30, the clearinghouse server 20, the media recording device 15, and the media playing device 80 interact within the constraints of licensing from content owners to provide means for the user to play content 35 on the media playing device 80 or make a legal copy of content 35 on the physical media 65.

[0032] The block diagram of FIG. 2 illustrates a high-level architecture of the title key protection system 10. The title key protection system 10 comprises a content preparation utility 205 in the content repository 25 media recording device and a title key decryption/encryption module 215 on the clearinghouse server 20. The content repository server 30 provides content 35 to the media recording device 15 in the form of an encrypted content/title key package 220. The media recording device 15 comprises a title key processing module 210. The media recording device 15 extracts the encrypted title key 225 from the encrypted content/title key package 220.

[0033] The media recording device 15 provides to the title key decryption/encryption module 215 the media key block 70, the media ID 75, and the encrypted title key 225. The title key decryption/encryption module 215 extracts a media unique key from the media key block 70 and the media ID 75. The title key decryption/encryption module 215 then decrypts the encrypted title

key 225 and re-encrypts it using the media unique key, creating a re-encrypted title key 230 that is unique to physical media 65. The clearinghouse server 20 returns the re-encrypted title key 230 to the media recording device 15 for burning on the physical media 65 with content 35.

[0034] A method 300 for obtaining the re-encrypted title key 230 for media recording device recording content 35 onto the physical media 65 for later playing by media playing device 80 is illustrated by the process flow chart of FIG. 3 (FIGS. 3A, 3B). At step 305, the content preparation utility 205 prepares recordable media such as content 35 by encrypting content 35 with a title key. The title key may, for example, be randomly selected. The title key is encrypted with content 35 in a manner agreed upon between the clearinghouse 40 and the content repository 25, creating an encrypted content/title key package 220.

[0035] All methods for encrypting the title key with content 35 are within the scope of the title key protection system 10. Exemplary encryption methods comprise the use of a common key agreed upon between the clearinghouse 40 and the content repository 25, the use of a public key provided by the clearinghouse server 20, and the use of a key from a media key block.

[0036] The content repository server 30 stores the encrypted content/title key package 220 at step 310. The title key is encrypted and packaged with content 35 that has been encrypted by the content preparation utility 205 and stored as one transparent encrypted entity in the content repository 25. By storing the content 35 and the title key in encrypted form in the content repository 25, the content repository 25 needs no tamper-resistant storage to protect the title key.

[0037] The user accesses the content repository server 30 at step 315 and obtains content 35. Content 35 may be provided for purchase, rent, or for free to the user by the content repository 25. The content repository server 30 responds to the request and transmits the encrypted content/title key package 220 to the media recording device 15 at step 320. The title key processing module 210 extracts an encrypted title key 225 from the encrypted content/title key package 220.

[0038] The media recording device 15 transmits the media key block 70, the media ID 75, and the encrypted title key 225 to the clearinghouse server 20 at step 330. The title key decryption/encryption module 215 decrypts the encrypted title key 225 at step 335 in a cryptographic protocol pre-arranged the content repository 25. The title key decryption/encryption module 215 derives a media unique key at step 340 from the media key block 70 and the media ID 75. At step 345, the title key decryption/encryption module 215 encrypts the title key in the media unique key, creating a re-encrypted title key 230. The clearinghouse server 20 transmits the re-encrypted title key 230 to the media recording device 15 at step 350. The media recording device 15 records the content 35 and the re-encrypted title key 230 on the physical media 65 at step 355. The media can now be played on media playing device 80.

[0039] In an embodiment, step 330 may be modified as illustrated in FIG. 4 to minimize the amount of data transmitted on average from the media recording device 15 to the clearinghouse server 20. The media key blocks 70 are mass-produced. For example, a single media key block 70 may be pressed into up to a million DVD recordable blank discs. Consequently, it is very likely that any given media key block 70 has already been seen by the clearinghouse 40 from a previous transaction.

[0040] The media recording device 15 transmits a short digest of the media key block 70 to the clearinghouse server 20 at step 405 in addition to the media ID 75 and the encrypted title key 225. The title key decryption/encryption module 215 determines at decision step 410 whether the media key block 70 has been previously seen. If yes, the title key decryption/encryption module 215 uses the previously seen media key block 70 at step 415. If no, the title key decryption/encryption module 215 requests the media key block 70 from the media recording device 15 at step 420. The media recording device 15 transmits the media key block 70 to the clearinghouse server 20 at step 425. In an embodiment, the verification data in bytes 5 through 12 of the media key block 70 uniquely identifies the media key block 70 and can be sent as the digest. However, all techniques of making a digest such as, for example, a cryptographic hash of the media key block 70, are within the scope of the title key processing module system 210.

[0041] It is to be understood that the specific embodiments of the invention that have been described are merely illustrative of certain applications of the principle of the present invention. Numerous modifications may be made to a system and method for protecting a title key in a secure distribution system for recordable media content described herein without departing from the spirit and scope of the present invention. Moreover, while the present invention is described for illustration purpose only in relation to the WWW, it should be clear that the invention is applicable as well, for example, to an intranet, a wide area network, or any other network in which devices may interconnected for communications purposes.